ELECTRONIC AUTHENTICATION POLICY WORKSHOP

Working Papers

Industry Canada
November 22, 1999

ELECTRONIC AUTHENTICATION POLICY WORKSHOP
Working Paper

PANEL 1: Market Development - Opportunities and Challenges

Moderator: Mr. Wayne Scott
Government Programs, IBM Canada Ltd.

This paper has been prepared to facilitate and stimulate discussion at the first panel discussion at the Workshop. It is intended as a starting point for a dialogue on identifying strategic initiatives that can be undertaken to develop and promote the authentication and services market. The paper will continue to evolve as it incorporates further input received from additional stakeholders, helping to ensure its continued relevance to dynamic market conditions.

At the Workshop, input will be sought on what participants believe should be the elements of a strategy to guide and promote the development and use of authentication services in Canada, taking into account the input received from the initial round of consultations. Industry Canada's current perspective is that a strategy should:

- **accelerate innovation in technologies and applications;**
- **address barriers to entry and impediments to investment;**
- **promote the adoption of services by end users (business and consumers); and,**
- **expand domestic and international opportunities for suppliers and end users.**

The paper proposes some measures to help meet the objectives. As a first step, discussion at the Workshop could focus on:

- **assessing the opportunities for Canadian businesses in the authentication market;**
- **identifying and exploring the significance of impediments for suppliers and end users;**
- **assessing the risks to the marketplace in terms of forfeited growth by not having a coherent approach; and finally,**
- **suggesting appropriate strategic initiatives to mitigate the risks and capture the opportunities.**

Industry Canada
November 22, 1999

CANADIAN MARKET DEVELOPMENT OPPORTUNITIES AND CHALLENGES

Introduction

It is generally recognized that Canada has a strong and rapidly growing high-technology sector and that domestic and international market opportunities for Canadian companies are growing as electronic commerce becomes widespread. Electronic authentication service providers create confidence and play an important role in the Canadian e-commerce agenda by providing security, and confidentiality for businesses and consumers. Since there are some Canadian companies and associations developing and promoting world-class solutions to protect sensitive information and communications travelling across an increasingly diverse infrastructure, Canada is already a significant player in the security segment of the electronic commerce market.

As such, Canada has the opportunity to become a world leader in the development and use of authentication and certification services and to enjoy the corresponding jobs and growth benefits that will accrue to all stakeholders. However, in order to achieve this, there is a need to have a domestic approach to the development and use of these services that will help position Canada internationally, or we will lose some of the opportunities that would be available.

We need to look for ways to monitor changing market conditions, grow new services and strengthen the competitive position of both large and small Canadian businesses in this environment. The Federal Government has provided some parameters for this new marketplace by expressly supporting an industry-led approach to the development of authentication products and services and clarifying its intention to not introduce licensing requirements for CAs.[1]

In the context of the initial stakeholder consultations that have already taken place[2], private sector representatives expressed support for the Government's decision to adopt a market-oriented approach but suggested that the relative roles and responsibilities of the public and private sectors required further discussion. Recognizing that technology challenges associated with the millennium are largely behind us, strategies can be put in place to capitalize on Canada's advantages in this market.

---

[1] Announced by the Minister of Industry in October 1998 in the context of the Cryptography Policy.

[2] *Electronic Authentication: Summary Findings of Bilateral Consultations* (October 1999).

Strategic Objectives

Input received during the first round of consultations confirmed that if Canada is to exploit domestic and international market opportunities, a strategy that addresses the needs of all stakeholders (suppliers and business/consumer end users) needs to be developed with overarching principles and objectives articulated. It is understood that such a strategy would be of an evolving nature to reflect continuing dialogue among stakeholders and changing market conditions.

Taking into account input received from the initial stakeholder consultations, Industry Canada's current perspective is that a strategy should:

- accelerate innovation in technologies and applications;
- address barriers to entry and impediments to investment;
- promote the adoption of services by end users (business and consumers); and,
- expand domestic and international opportunities for suppliers and end users.

Addressing the Objectives

Any market development strategy would need to identify the drivers and inhibitors to investment in security solutions that involve authentication and certification services. **What does Canada need to do if it wants to take a lead in the supply and use of these services? Is there a need to establish some kind of framework to guide the development of electronic authentication services to enhance investment and provide some direction for innovation? Should the emphasis be on business-to-business with efforts focussed on ensuring there are ways for business to establish trusted relationships with each other at both the national and international level? What emphasis should be placed on business-to-consumers?**

In examining this market and identifying the steps to promote its development, there may be merit in undertaking some analysis to assess the market for authentication and certification products and services and identify who is providing them. Emerging trends in the marketplace indicate that adoption rates of user authentication vary significantly across industry sectors. Those with lower rates could be identified and initiatives introduced to increase the usage in the industries involved.

a) <u>International Factors</u>

Canada's continued involvement in various international fora addressing authentication is critical to ensuring the global acceptance and use of Canadian products and services with no barriers to trade. There is a need to ensure that Canadian approaches are compatible with those of trading partners and are not trade restrictive. Any failure to meet international norms could restrict Canada's trade with other countries and result in transborder blockages. In this regard, continued

close collaboration between the federal government and industry is central to Canada's active participation in the economic policy work of the Organization for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC) and other fora. **Are there ways to enhance Canada's current contribution to these initiatives? How can we raise the visibility of our suppliers and service providers (including those offering intermediary services) and have a stronger influence on international directions? Should we be taking a partnership (technologies, suppliers, governments) approach and, if so, with what countries? What opportunities are there for Canada to take a leadership role in developing and establishing international standards?**

b) Domestic Factors

In the context of the bilateral consultations, stakeholders have observed that the authentication and certification services market is nascent with few suppliers and limited competition. On this basis, there was strong endorsement for Industry Canada's technology-neutral approach. It was also observed that this market offers new opportunities to some business sectors. For example, players not previously involved in certain aspects of electronic commerce can utilize this technology to offer new services and assume new roles. **In this connection, how can competition and innovation be fostered?**

Small and medium-sized businesses are looking for the development of readily available, reasonably priced products. Consumers are seeking user-friendly tools to provide them with assurances related to the identity of the parties with whom they are doing business and the integrity of transactions in this environment. Authentication and certification services can provide the security, confidentiality and trust that both business and consumers are demanding. As such, there is a need to promote, and ensure the availability of, authentication products and services to meet this demand. To this end, there may be synergies possible with existing initiatives such as the "Canadian E-Business Opportunities Roundtable"[3] that brought together public and private sector representatives to develop a set of national initiatives on e-business development. Specific proposals have arisen from this process that could include components aimed at promoting Canadian authentication products and services. For example: the creation of a specialized group of e-business suppliers to promote the importance and advantages of authentication services domestically, and to potential foreign investors; the development of high-tech "clusters" focused on authentication to provide for co-operation between universities, established anchor companies and early-stage capital providers to foster innovation and, subsequently economic growth; and, the recognition of the role for governments in taking a leader ship role as model users. Seizing opportunities to influence directions in the various international standardization fora would also be important.

An additional consideration in exploiting the opportunities that exist for Canada, will be the need

[3] Organized by the Boston Consulting Group (BCG) and supported by Industry Canada and the private sector.

to have continuity across the provinces so that a patchwork of approaches does not emerge that would be costly and burdensome domestically, and an inhibitor to the ability of Canada's service providers to interoperate globally.

What are the respective roles of the public and private sectors in developing and implementing a strategy for the domestic market? Do they differ according to whether the focus is business-to-business or business-to-consumer? Should the emphasis be on getting the domestic environment right and then move outward and influence international directions or should we focus on international initiatives and follow with defining a compatible domestic strategy? How important is it for provincial approaches to be compatible within Canada?

Potential Next Steps

In discussing any next steps, there is a need to identify the threats and opportunities, define concrete action steps and determine the respective roles of the marketplace and governments in addressing them. In the interest of making effective and efficient use of resources and avoiding duplication of effort, there is also a need to make a concerted effort to keep apprised of relevant initiatives and identify areas where opportunities are available and synergies are possible.

In looking forward, if we are to exploit market opportunities in this area, there is a need to find ways to ensure that:

- any barriers to the deployment and use of private sector authentication services are addressed;
- Canadian suppliers face a level playing field and are not at a disadvantage vis-a-vis their competitors from other countries;
- Canadian electronic authentication services are available for both business and consumers by identifying and dealing with any barriers that may be in the way of broader diffusion of secure e-commerce services; and,
- international trade and investment opportunities for Canadian companies are fully explored.

ELECTRONIC AUTHENTICATION POLICY WORKSHOP

Working Paper

PANEL 2: Approaches to Self-Regulatory Accreditation Schemes

Moderator: Mr. Michael Geist
Professor of Law, University of Ottawa

This paper has been prepared to facilitate and stimulate discussion on the various approaches available to self-regulatory schemes. In choosing any option(s) for adoption in Canada, each must be assessed from the perspective of the degree to the which they are likely to meet appropriate marketplace principles. Industry Canada and stakeholders have suggested some basic principles in the initial round of consultations. Workshop participants will be asked to confirm these and possibly others as the basis for evaluating the accreditation models.

The range of approaches to self-regulatory accreditation schemes can be viewed on a continuum. This paper outlines the options at the two ends of the continuum and then describes some of the alternatives in between. The paper is not exhaustive in its survey of the potential options available. It recognizes that variations of the options employing elements of more than one approach may be possible. It also recognizes that, in order to meet the needs of the marketplace for a range of trust models, the co-existence of more than one scheme may be desirable.

At the Workshop, discussion will focus on evaluating the options and then identifying those that might be appropriate for the Canadian marketplace.

Industry Canada
November 22, 1999

APPROACHES TO SELF-REGULATORY ACCREDITATION SCHEMES

Principles for Self-regulatory Accreditation Schemes

In October 1998, the Minister of Industry announced the details of the Government's cryptography policy. The Government rejected the idea of mandatory licensing of certification authorities and instead, indicated that it intends to encourage and support industry-led accreditation of private sector certification authorities as a means of promoting sound business practices and building consumer confidence.

Following on this announcement, Industry Canada began to explore the various options available for self-regulatory accreditation schemes. In doing so, it began by setting out some principles to guide its work in the area of electronic authentication and certification services. In brief, they relate to:

Principle	Desired Outcome
1) Privacy	development and use of privacy-respecting authentication services
2) Choice, trust and confidence	encouraging competition
3) Market-driven development	industry-led accreditation schemes
4) Jobs and growth in Canada	ensuring a fair marketplace with no barriers to investment
5) Interoperable infrastructures	establishing formal trust relationships between certification authorities (CAs)
6) Domestic harmonization	compatible federal and provincial requirements
7) Canadian certificates recognized globally	compatibility with international directions

These principles were discussed with stakeholders in the preliminary bilateral discussions that have already taken place and the common views expressed are outlined in the summary report[1] of these initial consultations. Essentially, while opinions varied across category of stakeholders and across industry sectors on the relative importance of each, there was broad consensus that the principles Industry Canada had adopted represented a good starting point for discussion.[2]

---

[1] *Electronic Authentication: Summary of Findings of Bilateral Consultations* (October 1999).

[2] It was acknowledged that the principles may need to be revisited in the context of certain business models and perhaps in light of national or international market developments.

International Context

There is a range of approaches to the authentication and certification environment internationally. The *Inventory of Approaches to Authentication and Certification in a Global Networked Society*[3] provides an excellent summary of this range in that the various Organization for Economic Co-operation and Development (OECD) member country approaches are detailed in the document. The international range varies from having:

a) open or closed CAs with no formal recognition;
b) contractual relationships;
c) voluntary accreditation by non-governmental body;
d) voluntary licensing of CAs;
e) mandatory licensing of CAs; and finally,
f) legislation requiring mandatory use of state-operated CAs.

Given the Federal Government has already announced that it would not implement any form of licensing scheme for certification authorities, from a federal perspective, certain of these options have already been rejected. However, it is important to understand the international context within which the Canadian self-regulatory approach would function and need to interoperate (i.e., across jurisdictions with different approaches) and to be aware of the array of mechanisms that are currently being employed in this marketplace.[4]

Approaches to Meeting the Principles

a) Laissez-faire

The options available can be viewed on a continuum or spectrum with a complete laissez-faire approach at one end that would involve leaving the arena wide open. Under such an approach, existing consumer protection measures and contract law would presumably apply. New initiatives would not be introduced except to update existing law and policy on an "as required" basis. Proponents of this approach would argue that if market forces are allowed to work as they should, Canadians will benefit from greater choice and lower prices.

---

[3] Prepared by the Organization for Economic Co-operation and Development (OECD) Committee for Information, Computer and Communications Policy within the Science, Technology and Industry Directorate (October 1999).

[4] While the federal government has indicated it will not pursue a licensing approach, the provinces have not as yet done likewise. As such, it is currently theoretically possible for Canada to end up with a mix of licensed and unlicensed CAs (as with the UK) if one of more provincial governments decided to introduce licensing conditions for CAs within their jurisdiction.

However, this approach raises questions as to whether businesses alone can provide the self-regulatory frameworks needed to interoperate internationally and to allocate equitably the responsibilities among the various parties to an authentication transaction. It also raises questions as to whether such an approach is the most desirable one to adopt if the environment is to evolve in such a way so as to maximize the opportunities and benefits for all parties. Under this approach, there is therefore a question as to whether other elements need to be put in place to ensure the trustworthiness and reliability of certification services, the equitable allocation of responsibilities, the ability for Canadian certificates to be recognized globally and the ability for all parties to realize the maximum benefit.

b) Single Authority

At the other end of the spectrum, is the establishment of a single authentication authority that offers authentication and certification services that adhere to strict government sanctioned standards and practices. For reasons related to Canada's cultural preferences on the one hand, and federal/provincial dimensions on the other, it is likely that both extremes are unacceptable and that the range of options available between should therefore be explored.

The options in between:

While the potential options and available mechanisms lying in between the two extremes are numerous and diverse, most alternatives would likely involve either the development and implementation of some form of minimum standards of practice for CAs or the establishment of one or more accreditation schemes. It is possible that the most desirable approach may involve elements of both.[5] It is also possible that the approaches could co-exist so that a range of trust models is available to address the diverse security requirements of different applications in the various business environments[6] (although the implications of perhaps creating "classes" of services and transactions would need to be fully explored).

---

[5] A standards-based approach may also be used in combination with an accreditation approach in that standards can provide a basis to facilitate the "accreditation", or the measure of trustworthiness (in the case of public key approaches, the extent to which you can be sure a certificate truly binds a public key to an entity) of a CA.

[6] Entities will need to develop and manage their own security policies in the context of the their own threat and risk analysis.

a) Standards-based Approach

There are many factors supporting a standards-based approach. Multiple, independent closed community CAs can become costly and complex to administer and could limit the potential for information interchange involving multiple independent organizations. A common approach to the development of, for example, Certificate Policies[7], and the availability of related standards could help facilitate mutual recognition of electronic signatures generated within different policy domains and legal jurisdictions. It would appear that consumers would welcome such a common framework as it would enable them to make meaningful comparisons and therefore, informed choices about with whom they do business. The development of commercially viable standards would likely also result in the necessary commonality to provide for the level of harmonization needed to accommodate the interoperability that consumers are likely to expect.

To provide for added assurances aimed at protecting and preserving the public interest under such an approach, the standards developed could be formally recognized by governments. A federally sanctioned list of certification authorities that adhere to the standards might help consumers in making difficult choices and reduce uncertainty.

While standards can promote open and fair competition, there would be a need to ensure that they did not result in undue distortion of the market or impede innovation. On this basis, it is generally agreed that any standards must be private sector-led to ensure they are relevant, effective and reflect consensual agreements among users. Under this (and all) approaches, there would be questions as to timing and scope. **Should the approach be to wait for more market experience? Or, should Canada take a proactive approach and begin now to develop standards of some form to minimize costly retro-fitting of systems at some later date? Should the approach be to develop minimum standards for use in open environments? Would they apply to closed environments where parties are bound by pre-existing contractual rules and procedures?**

b) Accreditation

While the development of a set of standards would have obvious benefits, some would argue that it will be very difficult to establish the levels of trust we know are going to be necessary in this

[7] The Certificate Practice Statement would allow for independent implementations of the common policy.

environment without some level of accreditation. Developing a scheme for the accreditation of CAs would involve the interaction of a variety of players, each having responsibility for one or more aspects of the scheme depending on the unique accreditation model. It is possible that a number of accreditation schemes or models could be developed in response to a specific market need, tailored to address a well-defined requirement.

Whatever the exact form any accreditation model or scheme takes, it will need to be flexible enough to satisfy a variety of national or business requirements and implementation approaches. Generally though, their basic objective would be to formalize trustworthiness of the CAs across communities of interest. In doing so, they would presumably recognize the validity of contractual relationships within, and between, closed community CAs.

The scope of any accreditation model could vary. A very basic approach could simply ensure that the level of security, legal and performance requirements are effectively documented in the Certificate Policy; confirm through verification processes that the CA practices developed and documented in the Certificate Policy Statement comply with the requirements set out in the Certificate Policy; and, through compliance audits (or perhaps the levying of penalties), ensure that the CA follows disclosed practices. Other models could go further and incorporate mechanisms to evaluate schemes and mechanisms to "accredit" the evaluation mechanisms.

There are already tools that have been developed in the marketplace which could serve as a foundation for a common accreditation approach.[8] There are also various trusted product evaluation standards, organizations and programs that exist that could assist in the security certification and accreditation of certification authorities. For example, while website seals typically only indicate that general principles pertaining to business practices, transaction integrity and information privacy are followed, it might be useful to assess whether expanding any existing business/enterprise website accreditation model to include certification authority accreditation criteria (and utilizing the audit process performed by accounting bodies or other qualified professionals) is compatible to the needs of a CA accreditation process.

Alternatively, the necessary assurances about the players involved in any scheme could be derived from the establishment of a series of high-level "authentication authorities". Under this approach,

---

[8] For example, IETF (Internet Engineering Task Force) PKIX Part 4 *Certificate Policy and Certification Practices Framework* has a standard structure and check-list for listing Certificate Policy requirements for such aspects as certificate generation and revocation, maintenance of records etc. and for Certificate Practice Statements such as identity requirements, key generation, certificate issuance etc.

existing trusted bodies[9] could be established as authorities or such authorities could require some form of government approval.[10] Such a set of high-level authentication authorities could be involved in the accreditation of subsidiary service providers by providing a common certificate policy, ensuring compliance with practice statements and technical standards and facilitating cross-certification or mutual certification among other service providers. Given consumers appear to be looking for "transparency" (i.e., no requirement that they have a great deal of technical knowledge to use electronic authentication services), they may simply look to existing "trusted" bodies to provide them with the assurances they require in this environment. **However, such an approach raises fundamental questions as to whether it is appropriate for CA responsibility to be oligopolized by a small number of players or whether it should be competitively supplied by a number of vendors and trade associations to maximize choice in the marketplace.**

Next Steps

The foregoing is not intended to be an exhaustive look at available options for responses to this environment, but rather to serve as starting point for discussion. The various alternatives will need to be explored with a view to determining the best approach for the Canadian marketplace. The relative merits of the options need to be assessed according to the degree to which they meet the policy objectives. Such an assessment will be complicated by the fact that aspects of these policy objectives compete with one another. There will be challenges in arriving at an approach that achieves the right balance.

---

[9] There are existing professional bodies that could be used in CA accreditation schemes. Further work would be required to identify candidate bodies, their role, required qualifications and their relationship with government entities. The question of whether the marketplace should rely on existing trust infrastructures to provide the equivalence of accreditation would also need to be explored.

[10] Currently, there is a possibility that Canada will need some scheme with government involvement to provide for signatures to be legally binding in other jurisdictions (e.g., in the context of the *EU Directive on a common framework for electronic signatures).*

ELECTRONIC AUTHENTICATION POLICY WORKSHOP
Working Paper

PANEL 3: Public Policy Considerations

Moderator: Peter Ferguson

This paper has been prepared to facilitate and stimulate discussion of some of the public policy considerations that have been identified to date. For discussion purposes, the issues have been grouped into categories as follows:

Interoperability: the issues relate to the degree and extent of interoperation of authentication services that will be demanded by the marketplace and the operational aspects of how it can be achieved.

Legal and Risk: the issues relate to how liabilities will be allocated amongst the various parties to transactions and the need for disclosure.

Jurisdictional: the issues relate to the need for compatibility across provinces and internationally.

At the Workshop, the objective of the discussion will be to:

a) confirm that these issues require consideration
b) identify issues that have not been raised in the paper
c) priorize the issues
d) agree on appropriate response to them; and
e) determine private/public sector roles in addressing them.

Industry Canada
November 22, 1999

PUBLIC POLICY CONSIDERATIONS

Introduction

A number of public policy considerations were identified by Industry Canada in its initial work in the area of authentication and these were confirmed by stakeholders during the preliminary consultations that have already taken place.[1] However, it was acknowledged that, as this is new technology and a developing field, new considerations and issues will emerge as it evolves. There was general awareness that there are risks associated with imposing a specific direction or vision at this early stage in this market.

While the identified issues are highly inter-related and inter-dependent, and should therefore be explored in relation to each other, for discussion purposes they can be generally grouped into the categories listed below. The relative importance of each category will vary depending on stakeholder interests and perhaps by industry sectors. However, there is a need to arrive at some consensus concerning their ranking and therefore the areas where efforts should be focused to identify and implement appropriate responses.

In the area of **interoperability** the issues relate to the degree and extent that it will be demanded by the marketplace and the operational aspects of how it can be achieved. The **legal and risk** issues focus on how liabilities will be allocated amongst the various parties to secure transactions and the **jurisdictional** issues relate to the need to for compatibility across provinces and internationally.

Interoperability

Interoperability will create the conditions for the successful development of electronic commerce. Given the global nature of electronic commerce, it has become of increasing interest within the domestic and international technical and legal communities. However the problems and issues enabling certification authority (CA) interoperation are yet to be fully explored or even fully identified and the extent of the marketplace demand is, as yet, unknown.

A term encountered in the context of interoperability is cross-certification which has various

---

[1] *Electronic Authentication: Summary Findings of Bilateral Consultations* (October 1999).

interpretations in the literature but essentially involves the issuance of a certificate by one CA to another. More recently, the concept of mutual recognition has emerged which is a less rigorous approach providing for the certificates of one CA to be recognized as assured and trusted by another CA under some form of arrangement. In either case, it is the question of whether there should be a transference of trust that is being debated. The answer will likely vary depending on the applications and the requisite security requirements.

The greater the consistency among CAs, and the public key infrastructures within which they operate, the easier it will be to achieve and maintain their interoperation and the less legal uncertainty there will be. This would suggest that interoperation endeavours will likely, at least in the short term, occur within industry sectors where common security and business controls are likely to prevail. **However, is the development of standards to facilitate cross-industry interoperability desirable?**

In the absence of any international convention in this area, the various legal systems throughout the world have material differences that will challenge the interoperation among CAs located within different jurisdictions and make the development of contractual arrangements and the co-ordination of agreements and documents extremely difficult. As such, there is tremendous benefit in continuing Canada's active involvement in the various international and trading region initiatives that are examining the elements that must be put in place to provide an environment conducive to global interoperability of CAs. **In the context of these initiatives, should efforts aimed at incorporating mutual recognition provisions in both domestic and international frameworks for electronic authentication be the objective?**

Legal and Risk Issues

There will be a need to establish the rights and obligations of keyholders, certification authorities and relying parties in this environment. These will need to be well-defined and clearly allocated. In the case of such closed community CAs, where business relationships already exist, a set of self-contained rules can govern these relationships. Liability can be allocated by contractual arrangements. On the other hand, allocation of liability in open environments will present challenges. On this basis, discussions of liability will probably need to be differentiated on the basis of whether a closed or open model is involved. Distinctions may also need to be made on the basis of the level of assurance associated with the certificate (e.g., it has been suggested that there should be no CA liability in the case of low-value certificates). Limited market experience to date has meant that the risks are not yet fully discernable or measurable. However, the

American Bar Association Guidelines[1] provide a framework for discussion of this area and other legal aspects.

Regardless of the business model, all parties will need to understand that they have critical functions and obligations in the context of electronic authentication services. From a public policy perspective, the consumer dimension will perhaps be the most important. Specifically, consumers will need to understand that they have certain obligations to CAs (e.g., to co-operate in confirmation of identity and in some cases, to generate a private signing key etc.) and certain obligations to relying parties (to keep private signing keys safe[2], to provide timely notification of lost or stolen keys, to use certificates only for applications for which they are suited etc.).

As of yet, it is unclear what type of liability the consumer should bear in this environment. In the final analysis, it may only be tested against "reasonableness" concepts but the question as to whether it should be formalized in some way seems to warrant further discussion. **For example, in the case of the misuse or loss of the private signing key, should the consumer be liable in some way, and if so, how can the liability be clarified and quantified to the consumer? Disclosure requirements would play a role in these discussions. Other questions will relate to whether the liability should be limited, even in cases where it has been determined that the consumer has not acted reasonably. Where the court systems are involved, there will be questions as to whether authentication services are a "good" or a "service" (i.e., would the common law apply or the Uniform Commercial Code or other rules governing goods?).**

In a competitive market, consumers would choose CAs based on performance and cost that would, in most cases, be spelled out in a contract. However, given the array of technical, business and legal issues associated with the provision of CA services, the contracts in this environment are likely to be long and complex. This may place an unreasonable burden on the ability of consumers to analyse these contracts, properly distinguish between CAs and make rational choices. This will be further hindered by the potential need to refer to other lengthy documents such as the Certificate Policy and Certificate Practice Statement to understand, for example, the approach taken by the CA to mutual recognition arrangements or cross-certification. **Is there a need to develop default rules for this relationship? Could any such rules address concerns regarding consumers becoming parties to unnegotiated contracts? Would the uniformity**

---

[1] *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*. American Bar Association Information Security Committee, August 1996.

[2] Hardware token approaches (such as storing keys on smart cards etc.) can be introduced to facilitate an individual's ability to safeguard their keys and reduce the possibility of fraud but this could have cost implications to consumers if they are expected to buy the readers that would be required

and predictability they would bring to the marketplace be to everyone's benefit?

Given that CAs are in a position to accumulate a wealth of information on individual subscribers, there will also be privacy concerns expressed by consumers. To a large extent, these concerns will be addressed by pending legislation[3] that contains a range of measures to protect personal information and gives law enforcement agencies the legal framework they need to ensure public safety. However, the need for "privacy-respecting" services in this environment remains a challenge and a potential issue.

Governments probably have a role in educating and empowering the public to enhance awareness of their responsibilities and their ability to exercise choice with respect to their protection as consumers. The various public/private sector collaborative initiatives being undertaken by Industry Canada's Office of Consumer Affairs (OCA) in the area of electronic commerce[4] confirms that this has already been recognized and is being acted upon. Any initiatives undertaken to address security elements specifically would need to be co-ordinated with these OCA initiatives.

Jurisdictional Issues

The global nature of electronic commerce raises an array of jurisdictional issues. In the Canadian context, they are at the provincial, federal and international level and also arise through international associations and bodies.

From an international perspective, there seems to be little doubt that governments have a role to play in terms of facilitating electronic transactions across borders and enabling the emergence of borderless networks of CAs supporting non-discriminatory agreements that will provide for mutual recognition.

At the domestic level, there will be a need for compatability across provinces and internationally to provide for the interoperation that is necessary for national and international electronic commerce. Ideally, in Canada, there would be a co-ordinated approach that covers the entire private sector even though some segments are federally regulated while others fall under provincial jurisdiction. Organizations such as the Uniform Law Conference of Canada[5] and

---

[3] *Bill C-6: Personal Information Protection and Electronic Documents Act.*

[4] Notably the development and recent publication of *Principles for Consumer Protection in Electronic Commerce - A Canadian Framework.*

[5] The Council has developed the *Uniform Electronic Commerce Act* that is designed to implement the principles of the United Nations Model Law on Electronic Commerce in Canada.

initiatives of the Public Sector CIO Council[6] could be instrumental in working towards this objective. However, it is possible that any federal initiative in this area could be restricted to facilitating the development of authentication services to meet various needs (e.g., possibly to encourage provinces to recognize that closed community CAs should be permitted to operate under their existing contracts, to give effect to "low-value" certificates etc.).

Next Steps

In discussing these various issues, it will be necessary to assess the respective roles of the private and public sectors with a view to developing a potential forward agenda to identify the mechanisms and processes available to address them. The extent and nature of the role of each sector in addressing the issues will probably be a function of the type of CA (i.e., open, closed or hybrid).

For many of the issues, the question becomes how to strike a balance between the government role and market-based solutions. While many would argue that all aspects should be left to the market, in the event that private sector solutions fail, they would probably look to governments to step in. As such, there may be some benefit in at least exploring the range of regulatory responses available in the event they become necessary to put into play in a timely fashion.

[6] Made up of Canada's Chief Information Officers (CIOs) from the provinces, territories and the federal government.

REFERENCES

Panel 1

Minister Manley Outlines Canadian Cryptography Policy, October 1, 1998, Electronic Commerce Task Force, Industry Canada, http://e-com.ic.gc.ca/english/crypto/631d1.html

Panel 2

Inventory of Approaches to Authentication and Certification in a Global Networked Society, Organization for Economic Co-operation and Development (OECD), *http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/inv-auth_e.pdf*

Certification Policy and Certification Practices Framework, The Internet Engineering Task Force, *http://www.ietf.org/*

Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, Commission of the European Communities, *http://www.ispo.cec.be/eif/policy/com98297en.doc*

Panel 3

Digital Signature Guidelines, American Bar Association, http://www.abanet.org/scitech/scitechpubs.html

Bill C-6, *The Personal Information Protection and Electronic Documents Act*, Electronic Commerce Task Force, Industry Canada, *http://e-com.ic.gc.ca/english/privacy/632d1.html*

Principles of Consumer Protection for Electronic Commerce and Supporting Documentation, Office of Consumer Affairs, Industry Canada, http://strategis.ic.gc.ca/sc_consu/consaffairs/engdoc/oca.html

The Uniform Electronic Commerce Act, August 1999, Uniform Law Conference of Canada, *http://www.law.ualberta.ca/alri/ulc/current/euecafin.htm*

ATELIER SUR LES POLITIQUES EN MATIÈRE D'AUTHENTIFICATION ÉLECTRONIQUE

Documents de travail

Industrie Canada
Le 22 novembre 1999

ATELIER SUR LES POLITIQUES EN MATIÈRE D'AUTHENTIFICATION ÉLECTRONIQUE

Document de travail

GROUPE D'EXPERTS 1 : Développement du marché - défis et possibilités

Modérateur : M. Wayne Scott
Programmes gouvernementaux, IBM Canada Ltée

Le présent document a été préparé pour faciliter et stimuler la discussion du premier groupe d'experts de l'atelier. Il sert de point de départ d'un dialogue sur le repérage d'initiatives stratégiques que l'on peut lancer afin de développer et de promouvoir le marché de l'authentification et des services. Le document sera modifié à mesure qu'on y incorporera l'apport d'autres intervenants afin de s'assurer qu'il continue d'être pertinent compte tenu des conditions dynamiques du marché.

Dans le cadre de l'atelier, on demandera aux participants les éléments qui, à leur avis, devraient faire partie d'une stratégie visant à orienter et à promouvoir l'élaboration et l'utilisation de services d'authentification au Canada, compte tenu des commentaires provenant de la série initiale de consultations. Dans la perspective actuelle d'Industrie Canada, la stratégie devrait incorporer les éléments suivants :

- **accélérer l'innovation concernant les technologies et les applications;**
- **tenir compte des obstacles à l'entrée et des entraves à l'investissement;**
- **promouvoir l'adoption des services par les utilisateurs finals (entreprises et consommateurs);**
- **élargir les possibilités au pays et à l'étranger pour les fournisseurs et les utilisateurs finals.**

Les auteurs du document proposent certaines mesures en vue de faciliter l'atteinte des objectifs. Dans un premier temps, les discussions dans le cadre de l'atelier pourraient viser à :

- **évaluer les possibilités qui s'offrent aux entreprises canadiennes sur le marché de l'authentification;**
- **déterminer et explorer l'importance des obstacles pour les fournisseurs et les utilisateurs;**
- **évaluer les risques pour le marché en termes de croissance perdue par manque d'une approche cohérente;**
- **suggérer des initiatives stratégiques appropriées pour mitiger les risques et saisir les bonnes occasions.**

Industrie Canada
Le 22 novembre 1999

Développement du marché canadien - défis et possibilités

Introduction

Il est généralement reconnu que le Canada possède un secteur fort de haute technologie qui est en croissance rapide, et que les débouchés au pays et à l'étranger pour les entreprises canadiennes s'élargissent à mesure que le commerce électronique prend de l'ampleur. Les fournisseurs de services d'authentification gagnent la confiance des utilisateurs et jouent un rôle important dans le programme canadien de mise en oeuvre du commerce électronique en offrant aux entreprises et aux consommateurs la sécurité et la confidentialité des transactions. Étant donné qu'il existe déjà plusieurs sociétés et associations canadiennes travaillant à l'élaboration et à la promotion de solutions de calibre mondial visant à protéger les renseignements et les communications de nature délicate qui sont transmis dans une infrastructure de plus en plus diversifiée, le Canada est déjà l'un des intervenants importants du segment de sécurité du marché du commerce électronique.

À ce titre, le Canada à l'occasion de devenir l'un des chefs de file de l'élaboration et de l'utilisation de services d'authentification et de certification et de tirer profit des avantages correspondants en matière de création d'emplois et de croissance économique qui s'offriront à tous les intervenants. Toutefois, afin de saisir cette occasion, le Canada doit élaborer une approche nationale afin de développer et d'utiliser ces services qui l'aideront à se tailler une place sur ce marché international; sans cette approche, il perdra certains des débouchés possibles. Le Canada doit trouver des façons de surveiller les conditions changeantes du marché, de développer de nouveaux services et de renforcer la position concurrentielle des grandes et des petites entreprises dans cet environnement. Le gouvernement fédéral a fourni quelques paramètres pour ce nouveau marché en appuyant clairement une approche, dirigée par l'industrie, concernant le développement de produits et de services d'authentification et en précisant son intention de ne pas énoncer des exigences pour ce qui est des licences d'organismes de certification.[1]

Dans le contexte des consultations initiales déjà tenues avec les intervenants[2], les représentants du secteur privé ont appuyé la décision du gouvernement d'adopter une approche axée sur le marché, mais ils ont laissé entendre que les rôles et responsabilités relatives des secteurs public et privé devraient faire l'objet de discussions approfondies. En reconnaissant que nous avons relevé la plupart des défis technologiques associés au millénaire, nous pouvons mettre en place des stratégies visant à tirer profit des avantages que le Canada possède dans ce marché.

---

[1] Annoncé par le ministre de l'Industrie en octobre 1998 dans le contexte de la politique sur la cryptographie.

[2] « Authentification électronique : Consultations bilatérales - Sommaire des conclusions » (octobre 1999).

Objectifs stratégiques

Les commentaires reçus au cours de la première série de consultations ont confirmé que, si le Canada veut saisir les occasions offertes sur les marchés intérieurs et internationaux, il doit élaborer une stratégie qui tienne compte des besoins de tous les intéressés (fournisseurs et entreprises/consommateurs utilisant les systèmes) et qui énonce des principes et des objectifs obligatoires. Il est entendu que cette stratégie serait de nature évolutive afin de tenir compte du dialogue continu entre les intéressés et des conditions changeantes du marché.

En s'appuyant sur les commentaires fournis au cours des consultations initiales avec les intéressés, Industrie Canada a formulé son point de vue actuel selon lequel la stratégie devrait servir aux fins suivantes :

- accélérer l'innovation en matière de technologies et d'applications;
- tenir compte des obstacles à l'entrée et des entraves à l'investissement;
- promouvoir l'adoption des services par les utilisateurs finals (entreprises et consommateurs);
- élargir les possibilités au pays et à l'étranger pour les fournisseurs et les utilisateurs finals.

Réalisation des objectifs

Toute stratégie de développement du marché doit faire état des facteurs suscitant ou empêchant l'investissement dans des solutions en matière de sécurité qui font appel à des services d'authentification et de certification. **Que doit faire le Canada s'il veut prendre les devants quant à la prestation et l'utilisation de ces services? Faut-il établir une sorte de cadre pour orienter l'élaboration des services d'authentification électronique afin d'accroître l'investissement et de diriger l'innovation? Doit-on mettre l'accent sur les relations inter-entreprises afin de permettre aux sociétés d'établir des rapports de confiance entre elles tant au Canada qu'à l'échelle internationale? Quelle importance faut-il accorder aux relations entre les sociétés et les consommateurs?**

Lorsqu'on examine ce marché pour déterminer les mesures susceptibles de favoriser son développement, il peut être utile d'effectuer une analyse visant à évaluer le marché des produits et services d'authentification et de certification et à déterminer les fournisseurs. Les tendances naissantes du marché indiquent que le taux d'adoption des services d'authentification de l'utilisateur varie considérablement d'un secteur industriel à l'autre. On pourrait déterminer les secteurs à faible taux afin de lancer des projets visant à accroître l'utilisation dans les secteurs en question.

a) Facteurs internationaux

Le Canada doit continuer à participer aux divers forums internationaux portant sur l'authentification s'il veut assurer l'acceptation et l'utilisation, à l'échelle mondiale, des produits et services canadiens sans obstacles au commerce. Il doit alors s'assurer que ses méthodes sont compatibles avec celles de ses partenaires commerciaux et qu'elles n'imposent aucune limite au commerce. Toute omission de respecter les normes internationales pourrait restreindre les échanges du Canada avec d'autres pays et entraîner des blocages transfrontaliers. À cet égard, le gouvernement fédéral et l'industrie doivent poursuivre leur collaboration étroite afin de permettre au pays de participer activement à l'élaboration des politiques économiques de l'Organisation de Coopération et de Développement Économiques (OCDE), l'Organisation de coopération économique Asie-Pacifique (APEC) et d'autres forums. **Existe-t-il des moyens d'élargir la contribution actuelle du Canada à ces initiatives? Comment le pays peut-il accroître la visibilité de ses fournisseurs de services (dont les fournisseurs de services intermédiaires) et exercer une plus grande influence sur les directives applicables à l'échelle mondiale? Le Canada devrait-il établir des partenariats (technologies, fournisseurs, gouvernements) et, dans l'affirmative, avec quels pays? Quelles sont les possibilités pour le Canada de jouer un rôle de premier plan dans l'élaboration et l'instauration de normes internationales?**

b) Facteurs intérieurs

Dans le contexte des consultations bilatérales, les intéressés ont observé que le marché de l'authentification et de la certification est naissant, de sorte qu'il existe peu de fournisseurs et que la concurrence est limitée. Pour cette raison, l'approche technologiquement neutre d'Industrie Canada a été fortement appuyée. Les intéressés ont également observé que ce marché offre de nouvelles possibilités à certains secteurs. Par exemple, les intervenants qui n'ont pas encore participé à certains aspects du commerce électronique peuvent se servir de cette technologie pour offrir de nouveaux services et jouer des rôles nouveaux. **Dans ce contexte, comment peut-on encourager la concurrence et l'innovation?**

Les petites et moyennes entreprises cherchent à développer des produits faciles à obtenir et à prix raisonnable. Les consommateurs sont à la recherche d'outils conviviaux afin d'être rassurés quant à l'identité des parties avec lesquelles ils traitent et quant à l'intégrité des transactions dans cet environnement. Les services d'authentification et de certification peuvent fournir la sécurité, la confidentialité et la confiance demandées tant par les entreprises que par les consommateurs. Il existe donc un besoin de promouvoir et d'assurer la disponibilité de produits et de services d'authentification pour satisfaire cette demande. À cette fin, il est possible de créer des synergies avec des initiatives existantes telle que la *Canadian E-Business Opportunities Roundtable*[3] qui réunissait des représentants des secteurs public et privé dans le but d'élaborer une série de projets visant à développer le commerce électronique. De ce processus découlent des propositions précises susceptibles de comporter des éléments destinés à promouvoir les produits et services

[3] Organisée par le *Boston Consulting Group (BCG)* et appuyée par Industrie Canada et le secteur privé.

d'authentification canadiens. Par exemple : la création d'un groupe spécialisé de fournisseurs appelés à faire connaître l'importance et les avantages des services d'authentification à l'échelle du pays et auprès d'investisseurs étrangers potentiels; la création de grappes de haute technologie consacrées à l'authentification et ayant pour mandat d'encourager la collaboration entre universités, entreprises bien établies et fournisseurs de capitaux de démarrage afin de stimuler l'innovation et, par ricochet, la croissance économique; et la reconnaissance du rôle que jouent les gouvernements en tant qu'utilisateurs modèles. En outre, il serait important de saisir les occasions qui se présentent pour influencer l'orientation de l'évolution dans les divers forums internationaux.

Il y a lieu de tenir compte d'un autre facteur important pour profiter des occasions qui s'offrent au Canada : la nécessité d'assurer une continuité dans les provinces de façon à éviter une multitude d'approches qui seraient coûteuses et encombrantes pour l'ensemble du pays et qui entraveraient la capacité des fournisseurs de services canadiens d'exercer leurs activités à l'échelle mondiale.

Quels sont les rôles respectifs des secteurs public et privé dans l'élaboration et de la mise en oeuvre d'une stratégie pour le marché national? Sont-ils différents selon qu'il s'agit de relations inter-entreprises ou de rapports entre consommateurs et entreprises? Devrait-on mettre l'accent sur la mise au point de l'environnement national avant d'influencer l'orientation d'autres pays ou devrait-on se pencher d'abord sur des initiatives internationales avant de définir une stratégie nationale compatible? Quelle est l'importance de la compatibilité des approches provinciales au sein du Canada?

Prochaines mesures éventuelles

Pour discuter des prochaines mesures, il faut repérer les risques et les possibilités, définir des mesures concrètes et déterminer les rôles respectifs que le marché et les gouvernements jouent dans le suivi. Dans l'intérêt d'utiliser les ressources de manière efficace et efficiente et d'éviter le dédoublement, il faut également se concerter pour se tenir au courant de projets pertinents et repérer des secteurs où des occasions se présentent et où des synergies sont possibles.

Si nous voulons tirer profit des débouchés futurs dans ce domaine, il faut trouver les moyens pour s'assurer que les conditions suivantes sont remplies :

- tout obstacle à l'instauration et à l'utilisation de services d'authentification du secteur privé est pris en compte;
- les fournisseurs canadiens sont en présence de règles de jeu équitables et ne sont pas désavantagés par rapport à leurs concurrents de l'étranger;
- des services d'authentification canadiens sont offerts tant aux entreprises qu'aux consommateurs grâce au repérage et au franchissement de tout obstacle pouvant gêner la diffusion à grande échelle de services de commerce électronique sécuritaires;
- les possibilités de commerce et d'investissement à l'échelle internationale pour les entreprises canadiennes sont explorées à fond.

ATELIER SUR LES POLITIQUES EN MATIÈRE D'AUTHENTIFICATION ÉLECTRONIQUE

Document de travail

GROUPE D'EXPERTS 2 : Approches relatives aux régimes d'autoréglementation de l'accréditation

Modérateur : M. Michael Geist
Professeur de droit, Université d'Ottawa

Le présent document a été préparé pour faciliter et stimuler la discussion sur les diverses façons d'établir des régimes d'autoréglementation. Avant de choisir un modèle à adopter au Canada, il faut évaluer chacune des options en fonction de la mesure dans laquelle elle correspond aux principes pertinents du marché. Industrie Canada et les intervenants ont suggéré plusieurs principes fondamentaux au cours de la première série de consultations. On demandera aux participants à l'atelier de confirmer ces principes et peut-être d'autres considérations qui devraient servir à évaluer les modèles d'accréditation.

L'éventail des méthodes servant à établir des régimes d'autoréglementation de l'accréditation peut être considéré comme un continuum. Le présent document fait état des options situées au début et à la fin de ce continuum avant de décrire les autres méthodes. Le document ne présente pas un aperçu complet des options possibles. Il reconnaît qu'on peut varier les options en employant des éléments de plusieurs méthodes. Il admet en outre que, pour satisfaire les besoins du marché de disposer d'un éventail de modèles éprouvés, il peut être souhaitable d'accepter la coexistence de plusieurs régimes.

À l'atelier, la discussion portera sur l'évaluation des options et la détermination des mécanismes pertinents pour le marché canadien.

Industrie Canada
Le 22 novembre 1999

APPROCHES RELATIVES AUX RÉGIMES D'AUTORÉGLEMENTATION DE L'ACCRÉDITATION

Principes relatifs aux régimes d'autoréglementation de l'accréditation

En octobre 1998, le ministre de l'Industrie a rendu publics les détails de la politique du gouvernement en matière de cryptographie. Il a alors annoncé que le gouvernement avait rejeté l'idée de mettre sur pied un régime obligatoire d'attribution de licences en vue de régir les autorités de certification (AC), mais qu'il entendait plutôt encourager et aider l'industrie à se charger elle-même de l'accréditation des AC du secteur privé, et ce, en vue de favoriser l'adoption de saines pratiques d'affaires et l'instauration de la confiance chez les consommateurs.

Après cette annonce, Industrie Canada a commencé à examiner les diverses options qui s'offraient aux autorités gouvernementales afin de promouvoir la création de régimes d'autoréglementation. Dans la foulée, il a établi un certain nombre de principes visant à guider son travail dans le domaine des services d'authentification et de certification électroniques. Voici, brièvement, sur quoi portent les principes :

Principes	Résultat visé
1) Protection de la vie privée	créer et utiliser des services d'authentification respectant la vie privée
2) Choix et confiance	favoriser la concurrence
3) Expansion menée par le marché	régimes d'accréditation sous la gouverne de l'industrie
4) Emplois et croissance économique au Canada	garantir un marché équitable sans obstacles à l'investissement
5) Infrastructures interopérables	favoriser l'établissement de relations officielles fondées sur la confiance entre les autorités de certification (AC)
6) Harmonisation des cadres fédéraux et provinciaux	compatibilité des exigences fédérales et provinciales
7) Reconnaissance mondiale des certificats canadiens	compatibilité avec les orientations internationales

Les principes ont fait l'objet de discussions à l'occasion de consultations bilatérales préliminaires, dont les conclusions sont exposées dans un rapport sommaire[1]. Essentiellement, d'une catégorie à l'autre ou d'un secteur industriel à l'autre, les intervenants divergent d'opinion concernant

[1] *Authentification électronique : Consultations bilatérales - Sommaire des conclusions* (octobre 1999)

l'importance relative de chaque principe, mais ils sont généralement d'accord pour affirmer que les principes adoptés par Industrie Canada constituent un bon point de départ pour lancer les discussions.[2]

Contexte international

À l'échelle internationale, sont préconisées un éventail d'approches dans le domaine de l'authentification et de la certification électroniques. Le *Inventory of Approaches to Authentication and Certification in a Global Networked Society*[3], qui expose en détail les formules privilégiées par les divers pays membres de l'Organisation de Coopération et de Développement Économiques (OCDE)6, est un excellent résumé de cette gamme d'approches, dont voici les grandes lignes :

a) soit recourir à des AC ouvertes ou fermées, sans reconnaissance officielle;
b) soit établir des relations contractuelles;
c) soit faire appel à un corps non public pour l'accréditation volontaire;
d) soit mettre en place un régime volontaire d'attribution de licences à l'intention des AC;
e) soit mettre en place un régime obligatoire d'attribution de licences à l'intention des AC;
f) soit adopter une loi en vue d'exiger l'utilisation d'AC exploitées par l'État.

Comme le gouvernement fédéral a déjà annoncé qu'il n'entendait pas mettre en place de régime d'attribution de licences afin de régir les AC, il lui a fallu rejeter d'emblée certaines des options précitées. Cependant, il importe de bien comprendre le contexte international dans lequel s'inscrirait l'approche préconisée par le Canada et axée sur l'autoréglementation, qui devrait néanmoins être interopérable (c.-à-d. être compatible avec les différentes approches adoptées ailleurs dans le monde), et de tenir compte de la variété de mécanismes qui sont actuellement utilisés sur le marché.[4]

Approches possibles en vue de respecter les principes

a) Laissez-faire

Les options qui s'offrent aux autorités gouvernementales peuvent être considérées comme un continuum et se situent entre deux options extrêmes, dont la première est le laissez-faire complet,

---

[2] Il a été reconnu qu'il faudra peut-être revoir les principes dans le contexte de certains modèles d'affaires et à la lumière de l'évolution du marché à l'échelle nationale ou internationale.

[3] Préparé par le Comité de la politique de l'information, de l'informatique et des communications, de la Direction de la science, de la technologie et de l'industrie, de l'Organisation de Coopération et de Développement Économiques (OCDE).

[4] Le gouvernement fédéral a indiqué qu'il n'entendait pas adopter un modèle fondé sur l'attribution de licences, mais les provinces n'ont pas encore arrêté leur position. Il est donc théoriquement possible que le Canada (à l'instar du R.-U.) finisse par retrouver sur son territoire un mélange d'AC reconnues ou non par licence, advenant qu'au moins un gouvernement provincial décide de réglementer ainsi les AC.

c'est-à-dire laisser libre cours aux forces du marché. Dans un tel cadre, s'appliqueraient vraisemblablement les mesures de protection des consommateurs et le droit des contrats déjà en vigueur. Les autorités gouvernementales n'adopteraient pas de nouvelles mesures et se contenteraient de mettre à jour au besoin les lois et politiques pertinentes. Les tenants de cette approche feraient valoir que, si on laisse libre cours comme il convient aux forces du marché, les Canadiens profiteront d'un plus grand éventail de choix et de prix moins élevés.

Il n'en demeure pas moins que cette approche soulève des questions. Il y a en effet lieu de se demander si, à elles seules, les entreprises sont en mesure favoriser la mise en place des cadres d'autoréglementation nécessaires pour leur permettre d'interopérer avec les autres à l'échelle internationale et assurer la répartition équitable des responsabilités entre les diverses parties à une opération d'authentification. Il convient également de se demander si le « ne rien faire » est l'option qu'il est souhaitable d'adopter, et ce, d'autant plus si on vise à maximiser les possibilités et les avantages s'offrant à toutes les parties. Bref, faut-il ou non mettre en place d'autres éléments en vue d'assurer la fiabilité des services de certification, la répartition équitable des responsabilités, la reconnaissance des certificats canadiens à l'échelle mondiale et la maximisation des avantages pour toutes les parties.

b) Autorité unique

La seconde option extrême, c'est la création d'une autorité d'authentification unique, qui offrirait des services d'authentification et de certification respectant les normes et pratiques officielles strictes et assorties de sanctions. Pour des raisons liées aux préférences culturelles au Canada, d'une part, et aux dimensions des relations fédérales-provinciales, d'autre part, ces deux options extrêmes sont vraisemblablement inacceptables, d'où la nécessité d'étudier plus à fond les options situées entre les deux.

Les options entre les deux extrêmes :

Même si les options et les mécanismes qui s'offrent aux autorités gouvernementales sont nombreux et divers, il n'en demeure pas moins que la plupart des moyens d'action consisteront vraisemblablement soit en l'élaboration et en la mise en oeuvre de normes minimums de pratique pour les AC, soit en la création d'au moins un régime d'accréditation. Il est possible que l'approche la plus souhaitable consiste en des éléments provenant des deux moyens précités[5]. Il est aussi possible que co-existent les deux approches, de sorte que les intéressés puissent disposer d'une gamme de modèles de confiance permettant de satisfaire aux diverses exigences de sécurité des différentes applications dans les divers environnements de l'entreprise[6] (il faudrait vraisemblablement examiner minutieusement les incidences de la création possible de « catégories » de services et de transactions).

---

[5] Les autorités gouvernementales pourraient également décider d'adopter une approche fondée sur le recours à des normes, conjuguée à une approche préconisant l'accréditation. Les normes serviraient alors à faciliter l'« accréditation » ou à mesurer le degré de fiabilité (dans le cas d'une infrastructure à clé publique, la mesure dans laquelle vous pouvez être sûr qu'un certificat lie véritablement une clé publique à une entité) d'une AC.

[6] Les entités devront élaborer et gérer leurs propres politiques de sécurité dans le contexte de leur propre analyse des menaces et des risques.

a) Approche fondée sur des normes

Bon nombre de motifs militent en faveur de l'adoption d'une approche fondée sur des normes. La multiplication des collectivités d'AC fermées et indépendantes pourrait devenir coûteuse et complexe à administrer et limiter les possibilités d'échange de l'information entre des organismes indépendants multiples. L'adoption d'une approche commune en matière d'élaboration, par exemple, des politiques d'attribution des certificats[7] et l'existence de normes connexes contribueraient à faciliter la reconnaissance mutuelle des signatures numériques, et ce, quelle que soit leur provenance (différents domaines ou territoires). Vraisemblablement, les consommateurs accueilleraient favorablement l'adoption d'un tel cadre commun, vu qu'ils seraient ainsi en mesure de bien comparer les services et, par le fait même, de choisir de manière éclairée ceux avec qui ils souhaitent faire des affaires. Ils se réjouiraient aussi sans aucun doute de l'élaboration de normes viables commercialement et propres à assurer le niveau d'harmonisation nécessaire pour favoriser l'interopérabilité voulue.

En vue de bien protéger et préserver l'intérêt public dans un tel cadre, les autorités gouvernementales pourraient reconnaître officiellement les normes de ce genre. Pour sa part, en avalisant la liste des AC qui se conforment aux normes, le gouvernement fédéral pourrait aider les consommateurs à faire des choix difficiles et contribuer à réduire l'incertitude.

Bien que les normes puissent favoriser le libre jeu d'une concurrence équitable, il faudrait veiller à ce qu'elles n'entraînent pas une distorsion indue du marché ni n'entravent l'innovation. Il est généralement reconnu que, dans un tel contexte, il convient que le secteur privé soit à l'origine des normes pour qu'elles soient pertinentes et efficaces et reflètent le consensus recueilli auprès des utilisateurs. En fin de compte, quelle que soit l'approche préconisée, il y aura aussi lieu de se demander quand et dans quelle mesure il faudrait intervenir. **Serait-il préférable d'attendre que le marché acquiert plus d'expérience? Ou, est-ce que le Canada devrait adopter une démarche proactive et commencer à élaborer dès maintenant des normes en vue de réduire les coûts de restructuration des systèmes ultérieurement? Serait-il préférable plutôt d'élaborer des normes minimums à des fins d'utilisation dans des environnements ouverts? Est-ce qu'elles s'appliqueraient dans un environnement fermé où les parties seraient liées par des règles et procédures contractuelles préexistantes?**

b) Accréditation

Même s'il ne fait aucun doute que l'élaboration d'un ensemble de normes serait avantageux sur plusieurs plans, certains pourraient soutenir qu'il sera très difficile, sans un certain processus d'accréditation, d'instaurer le niveau de confiance voulu. La mise sur pied d'un régime d'accréditation des AC nécessiterait l'interaction d'un éventail d'intervenants, qui assumeraient la responsabilité d'un ou de plusieurs aspects du régime selon le modèle retenu. Il est possible qu'il faille créer un certain nombre de régimes ou modèles d'accréditation en vue de répondre aux besoins particuliers et bien définis du marché.

---

[7] Un énoncé des pratiques en matière d'attribution des certificats permettrait la mise en oeuvre indépendante de la politique commune.

Quelle que soit la forme que prendrait le modèle ou régime d'accréditation, il faudrait que celui-ci soit suffisamment souple pour satisfaire les différentes exigences d'ordre national et celles en matière d'affaires et de mise en oeuvre d'approches. En général, cependant, le modèle ou régime d'accréditation aurait pour objectif de base d'officialiser la fiabilité des AC d'une communauté d'intérêt à l'autre. Il reconnaîtrait vraisemblablement, par le fait même, la validité des relations contractuelles existant au sein, et entre, les collectivités d'AC fermées.

Bien sûr, la portée du modèle d'accréditation, quel qu'il soit, pourrait varier selon les circonstances. Fondamentalement, il faudrait que le modèle permettre de faire ce qui suit : veiller à ce que le niveau de sécurité et les exigences sur les plans juridique et du rendement soient bien documentés dans la politique d'attribution des certificats; confirmer, par la vérification, que les pratiques des AC, précisées et étayées dans l'énoncé des pratiques en matière d'attribution des certificats, sont conformes aux exigences exposées dans la politique d'attribution des certificats; faire en sorte, par des vérifications de conformité (ou l'imposition de sanctions), que les AC suivent les pratiques officielles. Il serait aussi possible d'aller plus loin et de prévoir des modèles visant à évaluer les régimes et modèles servant à « agréer » les mécanismes d'évaluation.

Il existe déjà, sur le marché, des outils qui pourraient servir de fondement à un modèle d'accréditation commun.[8] Il serait aussi possible de recourir aux divers programmes, normes et organismes d'évaluation de produits, déjà reconnus, aux fins de l'accréditation des AC. Par exemple, même si les sceaux des sites Web n'indiquent habituellement que sont suivis des principes généraux en matière de pratiques d'affaires, d'intégrité des transactions et de protection des renseignements personnels, il pourrait être utile d'évaluer si l'accroissement de la portée de tout modèle d'accréditation existant de sites Web d'affaires/d'entreprises, en vue d'ajouter des critères à des fins d'accréditation des AC (et d'utiliser le processus de vérification des corps comptables ou d'autres corps de professionnels qualifiés), est compatible ou non avec les besoins d'un processus d'accréditation des AC.

Parallèlement, il serait possible de créer un ensemble d'« autorités d'authentification » de haut niveau, qui auraient pour tâche de fournir les assurances nécessaires au sujet des parties à tout régime d'accréditation. Par exemple, des corps existants de confiance[9] pourraient se voir conférer les pouvoirs requis pour agir comme autorités d'authentification, ou encore, de telles autorités devraient obtenir l'approbation des organismes publics compétents.[10] Un tel ensemble d'autorités

---

[8] Par exemple, la « Partie 4 » du PKIX du IETF (Internet Engineering Task Force), *Certificate Policy and Certification Practice Framework*, propose une structure et une liste de vérification types des exigences que devrait comporter une politique d'attribution des certificats (délivrance et révocation du certificat, tenue de dossiers, etc.) ou un énoncé des pratiques en matière d'attribution des certificats (confirmation del'identité, génération de clés, délivrance des certificats, etc.).

[9] Il existe des corps professionnels auxquels on pourrait faire appel aux fins de l'accréditation des AC. Il faudrait approfondir la question, bien sûr, en vue de déterminer les corps candidats, leur rôle, les qualifications requises et leur relation avec les entités publiques. Il faudrait également se demander s'il convient que le marché ne compte que sur les infrastructures de confiance existantes pour fournir l'équivalence de l'accréditation.

[10] Actuellement, il est possible que le Canada ait besoin d'un régime comportant un volet public officiel pour que les signatures soient reconnues sur le plan juridique dans les autres pays (p. ex., dans le contexte de la directive de l'UE sur l'adoption d'un cadre commun pour les signatures électroniques).

d'authentification de haut niveau pourraient être chargées d'agréer les fournisseurs de services complémentaires, en favorisant l'adoption d'une politique commune en matière d'attribution de licences, en veillant ce que soient respectés les énoncés de pratiques et les normes techniques et en facilitant la certification réciproque ou mutuelle entre les autres fournisseurs de services. Comme les consommateurs semblent préférer la « transparence » (c.-à-d. qu'il ne soit pas nécessaire de posséder beaucoup de connaissances techniques pour utiliser des services d'authentification électronique), ils pourraient simplement se tourner vers les corps de « confiance » existants pour obtenir les assurances voulues. **Toutefois, une telle approche soulève des questions fondamentales : convient-il que les responsabilités touchant aux AC soient concentrées entre les mains d'un petit nombre de corps ou est-il préférable qu'elles soient assumées par un certain nombre de vendeurs et d'associations commerciales en vue de maximiser les choix qui s'offrent sur le marché et de favoriser, par le fait même, la concurrence?**

Prochaines étapes

Ce qui précède n'est pas un examen exhaustif des options qui s'offrent aux autorités gouvernementales, mais plutôt un exposé de situation visant à servir de point de départ aux discussions. Il faudra étudier plus à fond les diverses options en vue de déterminer l'approche qui convient le mieux au marché canadien. Afin d'établir la pertinence relative des différentes options, il faudra évaluer dans quelle mesure chacune contribue à l'atteinte des objectifs d'orientation. Ce qui compliquera une telle évaluation, c'est le fait que se font concurrence des aspects de ces objectifs. Il sera donc nécessaire de se dépasser en vue d'en arriver à une approche offrant l'équilibre voulu.

ATELIER SUR LES POLITIQUES EN MATIÈRE D'AUTHENTIFICATION ÉLECTRONIQUE

Document de travail

GROUPE D'EXPERTS 3 : Considérations relatives aux politiques gouvernementales

Modérateur : Peter Ferguson

Le présent document a été préparé pour faciliter et stimuler la discussion de quelques-unes des considérations relatives aux politiques gouvernementales, soulevées jusqu'ici. Aux fins de discussion, les questions ont été regroupées dans les catégories suivantes :

Interopérabilité : les questions portent sur le degré et l'étendue de l'interopération des services d'authentification qui sera exigé par le marché et sur les aspects opérationnels de l'obtention de ce degré.

Considérations juridiques et risques : les questions touchent à la répartition des responsabilités parmi les diverses parties aux transactions, et à la nécessité de divulguer de l'information.

Les autorités : les questions portent sur la nécessité d'obtenir la compatibilité entre les régimes des provinces et la compatibilité à l'échelle internationale.

À l'atelier, les objectifs de la discussion seront les suivants :

a) **confirmer qu'il faut examiner ces question**
b) **repérer les sujets qui n'ont pas été abordés dans le document de travail**
c) **établir les questions par ordre de priorité**
d) **décider de la bonne façon de les régler;**
e) **déterminer les rôles des secteurs public et privé dans le règlement des questions.**

Industrie Canada
Le 22 novembre 1999

CONSIDÉRATIONS RELATIVES AUX POLITIQUES GOUVERNEMENTALES

Introduction

Un certain nombre de considérations relatives à la politique gouvernementale ont été identifiées par Industrie Canada dans le cadre de ses travaux initiaux dans le domaine de l'authentification et confirmées par les intervenants au cours des consultations préliminaires qui ont déjà eu lieu.[1] Toutefois, on reconnaît, étant donné qu'il s'agit d'une nouvelle technologie et d'un secteur en développement, que de nouvelles considérations et questions feront surface à mesure qu'ils évolueront. On est généralement conscient qu'il y a des risques associés à l'imposition d'une orientation ou d'une vision particulière aussi précocement sur ce marché.

Bien que les questions identifiées soient étroitement reliées entre elles et interdépendantes et doivent donc être examinées en fonction les unes des autres, elles peuvent généralement, aux fins de discussion, être regroupées dans les catégories énumérées ci-dessous. L'importance relative de chaque catégorie variera selon les intérêts des intervenants et en fonction peut-être aussi des secteurs d'activité. Cependant, il importe d'en arriver à un certain consensus au sujet de leur ordre de priorité et, par conséquent, des secteurs où les efforts devraient être concentrés pour qu'il soit possible de cerner et de mettre en oeuvre les solutions qui conviennent.

En ce qui concerne l'**interopérabilité**, les questions ont trait à la mesure dans laquelle elle sera exigée par le marché et aux aspects opérationnels de sa réalisation. Les questions de **droit** et de **risques** sont axées sur la façon dont les responsabilités seront réparties entre les diverses parties pour assurer la sécurité des transactions tandis que les questions de **compétence** ont trait à la nécessité d'une compatibilité d'une province à l'autre et à l'échelle internationale.

Interopérabilité

L'interopérabilité créera les conditions propices au développement réussi du commerce électronique. En raison de sa nature mondiale, le commerce électronique présente de plus en plus d'intérêt pour les collectivités techniques et juridiques nationales et internationales. Cependant, les problèmes et les questions touchant l'interopération des autorités de certification (AC) n'ont pas encore été explorés à fond ni même complètement identifiés, et l'étendue de la demande du marché demeure encore inconnue.

Un terme rencontré dans le contexte de l'interopérabilité est la certification réciproque, dont on trouve différentes interprétations dans la documentation, mais qui comporte essentiellement l'attribution d'un certificat par une AC à une autre. Plus récemment, le concept de la reconnaissance mutuelle a fait son apparition, lequel consiste en une approche moins rigoureuse selon laquelle les certificats d'une AC sont reconnus comme dignes de confiance par une autre en vertu d'un arrangement quelconque. Dans un cas comme dans l'autre, la question est de savoir s'il devrait y avoir un transfert de confiance. La réponse variera vraisemblablement en fonction des applications et des exigences requises en matière de sécurité.

---

[1] « Authentification électronique : Consultations bilatérales - Sommaire des conclusions » (octobre 1999).

Plus grande sera l'uniformité entre les AC et les infrastructures de sécurité à clés publiques à l'intérieur desquelles elles fonctionnent, plus facile il sera de réaliser et de maintenir leur interopération et moins grande sera l'incertitude sur le plan juridique. Cela donne à penser qu'il pourrait y avoir, du moins à court terme, plus de tentatives d'interopération dans des secteurs d'activité où des contrôles de sécurité et d'entreprise communs ont vraisemblablement cours. **Toutefois, l'élaboration de normes pour faciliter l'interopérabilité à l'échelle de l'industrie est-elle souhaitable?**

En l'absence de toute convention internationale en la matière, les différences matérielles entre les divers systèmes juridiques qui existent dans le monde constitueront un défi pour l'interopération des AC de territoires différents et compliqueront extrêmement l'élaboration d'arrangements contractuels et la coordination des ententes et des documents. C'est pourquoi le Canada aurait tout intérêt à continuer de jouer un rôle actif au sein des différentes tribunes internationales et commerciales régionales qui examinent les éléments qui doivent être mis en place pour assurer un environnement propice à l'interopérabilité mondiale des AC. **Dans le contexte de ces initiatives, les efforts visant l'incorporation de dispositions de reconnaissance mutuelle dans des cadres nationaux et internationaux pour l'authentification électronique devraient-ils être l'objectif?**

Considérations juridiques et risques

Il faudra préciser les droits et les obligations des détenteurs de clés, des autorités de certification et des parties utilisatrices dans cet environnement. Il est essentiel qu'ils soient bien définis et clairement répartis. Dans le cas des réseaux fermés où des relations d'affaires existent déjà entre les AC, un ensemble de règles internes pourra régir leurs rapports. La responsabilité pourra être attribuée en vertu d'accords contractuels. Par ailleurs, l'attribution de la responsabilité dans un environnement ouvert présentera des défis. C'est pourquoi les discussions entourant la responsabilité devront probablement être orientées selon qu'il s'agit d'un modèle fermé ou ouvert. Des distinctions pourraient également devoir être faites en fonction du niveau d'assurance associé au certificat (p. ex. il a été suggéré que la responsabilité des AC ne soit pas engagée dans le cas des certificats à prix modique). Parce que l'expérience du marché à ce jour est limitée, il n'est pas encore possible de discerner ou de mesurer pleinement les risques. Néanmoins, les lignes directrices de l'American Bar Association[2] fournissent un cadre pour la discussion de cette question et d'autres aspects juridiques.

Peu importe le modèle d'entreprise, toutes les parties devront comprendre qu'elles ont des fonctions et des obligations cruciales dans le contexte des services d'authentification électronique. Du point de vue de la politique gouvernementale, la dimension consommation sera peut-être la plus importante. Les consommateurs devront notamment comprendre qu'ils ont certaines obligations envers les AC (p. ex. coopérer pour que l'identité puisse être confirmée et, dans certains cas, générer une clé de signature privée, etc.) et envers les parties utilisatrices

---

[2] *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce,* American Bar Association, Information Security Committee, août 1996.

(assurer la sécurité des clés[3], signaler en temps opportun la perte ou le vol de clés, utiliser les certificats uniquement pour les applications auxquelles ils sont destinés, etc.).

Pour le moment, nul ne sait au sujet quel type de responsabilité le consommateur devrait assumer dans cet environnement. En dernière analyse, sa responsabilité ne peut être évaluée qu'en fonction du « caractère raisonnable », mais la question de savoir si elle devrait être officialisée de quelque manière que ce soit semble mériter une discussion plus poussée. **Par exemple, en cas de mauvaise utilisation ou de perte de la clé de signature privée, le consommateur devrait-il être tenu responsable en quelque sorte et, dans l'affirmative, comment clarifier et quantifier cette responsabilité du consommateur? Les exigences en matière de divulgation joueraient un rôle dans ces discussions. D'autres questions consisteront à savoir si la responsabilité devrait être limitée, même lorsqu'il a été déterminé que le consommateur n'a pas agi raisonnablement. Lorsque les tribunaux seront appelés à intervenir, ils auront à décider si les services d'authentification sont un « bien » ou un « service » (c'est-à-dire, est-ce que ce serait la *common law*, le Code commercial uniforme ou d'autres règles régissant les biens qui s'appliqueraient?).**

Sur un marché concurrentiel, les consommateurs choisiraient les AC en fonction du rendement et des coûts qui, dans la plupart des cas, seraient énoncés dans un contrat. Cependant, étant donné toute la gamme des questions techniques, commerciales et juridiques associées à la prestation des services des AC, il y a de grandes chances que les contrats soient longs et complexes. Cela pourrait constituer un fardeau déraisonnable pour les consommateurs de qui on exigerait qu'ils analysent ces contrats, distinguent les AC les unes des autres et fassent des choix rationnels. Les choses seront d'autant plus compliquées qu'ils pourraient devoir se reporter à d'autres documents volumineux comme la police de certification et l'énoncé des pratiques de certification pour comprendre, par exemple, l'approche adoptée par l'AC des arrangements de reconnaissance mutuelle ou de la certification réciproque. **Sera-t-il nécessaire d'établir des règles par défaut? De telles règles apaiseraient-elles les craintes que les consommateurs ne deviennent parties à des accords non négociés? L'uniformité et la prévisibilité qu'elles entraîneraient pour le marché seraient-elles avantageuses pour chacun?**

Étant donné que les AC sont en mesure d'accumuler toute une mine d'informations sur les différents abonnés, les consommateurs éprouveront des craintes à propos de la protection des renseignements personnels. Dans une large mesure, ces préoccupations seront réglées par la loi en voie d'adoption[4] qui renferme tout un train de mesures pour protéger les renseignements personnels et fournit aux organismes d'exécution le cadre législatif dont ils ont besoin pour assurer la sécurité du public. Néanmoins, la nécessité de services « respectueux de la vie privée » dans cet environnement demeure un défi et une source possible de problèmes.

---

[3] Des mesures (comme le stockage des clés sur des cartes intelligentes, etc.) pourraient être prises pour faciliter la protection des clés et réduire les possibilités de fraude, mais cela pourrait avoir des répercussions sur le plan des coûts pour les consommateurs s'ils devaient acheter les lecteurs requis.

[4] Projet de loi C-6 intitulé, *Loi sur la protection des renseignements personnels et les documents électroniques.*

Les gouvernements ont probablement un rôle à jouer pour ce qui est d'éduquer le public et de l'amener à prendre conscience de ses responsabilités et de sa capacité de faire des choix concernant sa protection. Les différentes initiatives de collaboration entre les secteurs public et privé entreprises par le Bureau de la consommation d'Industrie Canada dans le secteur du commerce électronique[5] confirment que le gouvernement a déjà reconnu cette nécessité et pris des mesures. Toutes les initiatives visant la sécurité plus particulièrement devraient être coordonnées avec celles du Bureau de la consommation.

Les autorités

La nature mondiale du commerce électronique soulève toute une gamme de questions de compétence. Dans le contexte canadien, ces questions se posent aux paliers provincial, fédéral et international et dans le cas également des associations et organismes internationaux.

D'un point de vue international, il ne fait presque aucun doute que les gouvernements ont un rôle à jouer s'agissant de faciliter les transactions électroniques transfrontalières et de permettre la création de réseaux sans frontière d'AC appuyant des accords non discriminatoires qui assureront la reconnaissance mutuelle.

Au niveau national, il faudra qu'il y ait compatibilité d'une province à l'autre et internationalement pour que l'interopération nécessaire au commerce électronique national et international soit possible. Idéalement, au Canada, il devrait y avoir une approche coordonnée qui englobe tout le secteur privé même si certains segments sont régis par le gouvernement fédéral tandis que d'autres relèvent de la compétence des provinces. Des organisations comme la Conférence sur l'uniformisation des lois du Canada[6] et les initiatives du Conseil des dirigeants principaux de l'information du secteur public pourraient aider à l'atteinte de cet objectif. Néanmoins, il est possible que toute initiative fédérale dans ce secteur soit restreinte à la facilitation du développement de services d'authentification pour répondre à divers besoins (p. ex. peut-être pour encourager les provinces à reconnaître que les AC en réseau fermé devraient être autorisées à fonctionner conformément à des contrats existants, rendre exécutoires les certificats « à prix modique », etc.).

Prochaines étapes

Dans le cadre de la discussion de ces diverses questions, il sera nécessaire d'évaluer les rôles respectifs des secteurs privé et public dans l'intention d'élaborer un programme d'action pour identifier les mécanismes et les processus dont on dispose pour faire face à la situation. L'étendue et la nature du rôle de chaque secteur à l'égard du règlement de ces questions seront probablement fonction du type d'AC (c.-à-d. ouverte, fermée ou hybride).

---

[5] Notamment la rédaction et la récente publication de *Principes régissant la protection des consommateurs dans le commerce électronique - Le cadre canadien.*

[6] Le Conseil a élaboré la *Loi uniforme sur le commerce électronique* qui est conçue pour mettre en application au Canada les principes de la loi type des Nations Unies sur le commerce électronique.

Dans le cas de bon nombre des questions, il s'agira de trouver un juste équilibre entre le rôle du gouvernement et les solutions axées sur le marché. Même si nombreux sont ceux qui pourraient croire que tous les aspects devraient être laissés aux forces du marché, si les solutions du secteur privé échouaient, on s'attendrait probablement à ce que les gouvernements interviennent. C'est pourquoi il serait peut-être souhaitable d'au moins examiner la gamme des réponses réglementaires possibles au cas où il pourrait s'avérer nécessaire d'intervenir en temps opportun.

Références

Groupe d'experts 1

CANADA. INDUSTRIE CANADA. *Le ministre Manley présente les grandes lignes de la politique du Canada en matière de cryptographie*, 1er octobre 1998. **http://ecom.ic.gc.ca/francais/crypto/631d1.html**

Groupe d'experts 2

FRANCE. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE (OCDE). *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, **http://www.oecd.org//dsti/sti/it/ec/act/Paris_ec/pdf/inv-auth_e.pdf**

THE INTERNET ENGINEERING TASK FORCE. *Certification Policy and Certification Practices Framework*, **http://www.ietf.org/**

BRUXELLES. COMMISSION DES COMMUNAUTÉS EUROPÉENNES. *Proposition de Directive au Parlement Européen et du Conseil sur un cadre commun pour les signatures électroniques*, 13 mai 1998, **http://www.ispo.cec.be/eif/policy/com98297fr.doc**

Groupe d'experts 3

ÉTATS-UNIES. AMERICAN BAR ASSOCIATION. *Digital Signature Guidelines*, **http://www.abanet.org/scitech/scitechpubs.html**

CANADA. INDUSTRIE CANADA. Le projet de Loi C-6, intitulé *Loi sur la protection des renseignements personnels et les documents électroniques26*, 26 octobre 1999, **http://ecom.ic.gc.ca/francais/privee/632d1.html**

CANADA. INDUSTRIE CANADA. Principes régissant la protection des consommateurs dans le commerce électronique et documents connexes, août 1999, **http://strategis.ic.gc.ca/SSGF/ca01180f.html**

CANADA. LA CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA. *Loi uniforme sur le Commerce électronique*, mars 1999, **http://www.law.ualberta.ca/alri/ulc/acts/fueca.htm**